Sums of Powers in Large Finite Fields: A Mix of Methods

Vitaly Bergelson, Andrew Best & Alex Iosevich

Published online: 23 Sep 2021.

Submit your article to this journal

Article views: 1510

View related articles

View Crossmark data
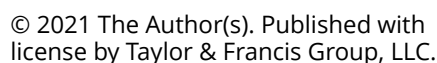
Sums of Powers in Large Finite Fields: A Mix of Methods

Vitaly Bergelson, Andrew Best, and Alex Iosevich

Abstract. Can any element in a sufficiently large finite field be represented as a sum of two dth powers in the field? In this article, we recount some of the history of this problem, touching on cyclotomy, Fermat's last theorem, and diagonal equations. Then, we offer two proofs, one new and elementary, and the other more classical, based on Fourier analysis and an application of a nontrivial estimate from the theory of finite fields. In context and juxtaposition, each will have its merits.

1. INTRODUCTION. We denote by $\mathbb{F}_q$ the finite field with q elements, where q is a power of a prime. Consider the following problem, which has been attacked several times in different centuries, and just two of its extensions.

Problem 1. Fix an integer $d > 1$. Show that for any sufficiently large finite field $\mathbb{F}_q$, we have

$$\mathbb{F}_q = \{x^d + y^d : x, y \in \mathbb{F}_q\},$$

or, in other words, every element of $\mathbb{F}_q$ is a sum of two dth powers.

Problem 2. Fix an integer $d > 1$. Show that for any sufficiently large finite field $\mathbb{F}_q$, we have for every $a, b \in \mathbb{F}_q^\times$ that

$$\mathbb{F}_q = \{ax^d + by^d : x, y \in \mathbb{F}_q\}.$$

Problem 3. Fix integers $n > 1$ and $k_1, \ldots, k_n > 0$. Given an element $b \in \mathbb{F}_q$ and coefficients $a_1, \ldots, a_n \in \mathbb{F}_q^\times$, determine the number of solutions $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$ to the *diagonal equation*

$$a_1 x_1^{k_1} + \cdots + a_n x_n^{k_n} = b. \tag{1}$$

Remarks. 1. Looking at Problems 1 and 2 with fresh eyes, one might first observe that since $x^{q-1} = 1$ for all $x \in \mathbb{F}_q^\times$, it follows that $\{x^{q-1} + y^{q-1} : x, y \in \mathbb{F}_q\} = \{0, 1, 2\}$, which is usually not all of $\mathbb{F}_q$. Thus, one should expect to require $q > d + 1$, hence the "sufficiently large" in the formulation. As we will see, in the case $d = 2$, this requirement is unnecessary.

2. The progression in difficulty of the problems should be clear, with Problem 3 a significant step up. Indeed, when $n = 2$ and $k_1 = k_2 = d$, knowing merely that the number of solutions to equation (1) is positive for each choice of a_1, a_2, b suffices to solve Problem 2. However, even the more modest jump from Problem 1 to Problem 2 can pose a challenge in that some approaches that work for the former seem unable to be easily upgraded to work for the latter.

3. According to Small, Kaplansky privately conjectured that the "outrageous" statement of Problem 1 holds [**28**]. We will see what role the article [**28**] occupies in the panoply of results we will survey shortly.

Mathematicians who have been caught on paper being interested in diagonal equations include Lagrange, H. M. Weber,[1] Cauchy, Skolem, Gauss, V. A. Lebesgue,[2] Dickson,[3] Hurwitz,[4] and Weil. In the process of proving his celebrated four-square theorem, Lagrange showed in [**19**] that, given any $b \in \mathbb{F}_p^\times$, we have $\mathbb{F}_p = \{x^2 + by^2 : x, y \in \mathbb{F}_p\}$. Though not the first to do so, Weber solved Problem 1 in the case $d = 2$:

Proposition 1 ([31, p. 309]). *Every element in a finite field $\mathbb{F}_q$ is the sum of two squares.*

Proof. Suppose $\mathbb{F}_q$ has characteristic 2, so that $q = 2^r$ for some positive integer r. Let $c \in \mathbb{F}_q$. Since $c^q = c$, it follows that $c = (c^{2^{r-1}})^2$, that is, c is a square. Thus, the element $c = (c^{2^{r-1}})^2 + 0^2$ is a sum of two squares.

Now suppose $\mathbb{F}_q$ has characteristic $p > 2$, with p prime. Let $c \in \mathbb{F}_q$. If c is already a square, there is nothing to show, so suppose c is a nonsquare. We now analyze two cases, depending on whether -1 is a square in $\mathbb{F}_q$. On the one hand, suppose -1 is a square in $\mathbb{F}_q$, so there is some element $g \in \mathbb{F}_q$ such that $g^2 = -1$. Then, the clever identity

$$c = \left(c + \frac{1}{4}\right)^2 + \left(g\left(c - \frac{1}{4}\right)\right)^2$$

expresses c as a sum of two squares. Note that when $p = 3$, the symbol $\frac{1}{4}$ means 1.

On the other hand, suppose $-1 = p - 1$ is a nonsquare in $\mathbb{F}_q$ instead. We always know that 1 is a square in $\mathbb{F}_q$. Now let's consider the prime subfield $\mathbb{F}_p \subseteq \mathbb{F}_q$, which is generated by 1. Since 1 is a square and $p - 1$ is a nonsquare, it follows that there is a pair of numbers a and $a + 1$, both in $\mathbb{F}_p$, and both nonzero, such that a is a square and $a + 1$ is a nonsquare. Since a is a square, there is a $g \in \mathbb{F}_q$ such that $g^2 = a$. Since c is a nonsquare and so is $\frac{1}{a+1}$, it follows[5] that $\frac{c}{a+1}$ is a square, so write $\frac{c}{a+1} = h^2$ for some $h \in \mathbb{F}_q$. We conclude that

$$c = \frac{c}{a + 1}(a + 1) = h^2(a + 1) = h^2 a + h^2 = (hg)^2 + h^2,$$

which shows that c is a sum of two squares. ∎

---

[1]Be careful with the initials. A contemporary of both the sociologist M. Weber and the physicist H. F. Weber, the latter of whose lectures' lack of Maxwell's equations spurred Einstein to spurn his mentorship, the mathematician H. M. Weber worked on algebra, analysis, and number theory, incorporating many of his results into his well-regarded textbook *Lehrbuch der Algebra*. According to Schappacher [**22**], Weber and Dedekind "[took] a decisive step towards the creation of modern algebraic geometry" with their publication of [**3**].

[2]Not the famous analyst!

[3]A prolific author, L. E. Dickson wrote (at least) two important books, namely the first comprehensive book on finite fields and the three-volume *History of the Theory of Numbers*. In a book review, he wrote, "Fricke's *Algebra* is a worthy successor to Weber's *Algebra*, which it henceforth displaces" [**7**].

[4]Here we write "Hurwitz" to mean the well-known A. Hurwitz, who collaborated with his generally overshadowed older brother J. Hurwitz on complex continued fractions.

[5]A short argument establishes that the product of two nonsquares is a square. The map $\phi : \mathbb{F}_q^\times \to \mathbb{F}_q^\times$ given by $\phi(x) = x^2$ is a group homomorphism with kernel $\ker(\phi) = \{1, -1\}$, so $H := \mathrm{im}(\phi)$ is an index 2 subgroup of $\mathbb{F}_q^\times$. In other words, $\mathbb{F}_q^\times / H$ is the group of two elements. As c and $\frac{1}{a+1}$ are nonsquares, we have $cH = \frac{1}{a+1}H$, hence $\frac{c}{a+1}H = (cH)(\frac{1}{a+1}H) = (cH)^2 = H$, hence $\frac{c}{a+1} \in H$.

© THE MATHEMATICAL ASSOCIATION OF AMERICA

Weber's proof amounts to cleverly producing, for each $c \in \mathbb{F}_q$, a solution to the diagonal equation $x^2 + y^2 = c$. It can be upgraded as follows to a solution to Problem 2 in the case $d = 2$:

Proposition 2. *For any finite field $\mathbb{F}_q$, we have for every $a, b \in \mathbb{F}_q^\times$ that*

$$\mathbb{F}_q = \{ax^2 + by^2 : x, y \in \mathbb{F}_q\}.$$

Proof. There are two cases. First, suppose that exactly one of a and b is a square, say a. If c is a square, then $\frac{c}{a}$ is a square, and hence $ax^2 = c$ has a solution in $\mathbb{F}_q$, which implies that $c \in \{ax^2 + by^2 : x, y \in \mathbb{F}_q\}$, and if c is a nonsquare, then similarly $bx^2 = c$ has a solution in $\mathbb{F}_q$, which implies the same. Second, suppose a and b are both squares or both nonsquares, so that $\frac{a}{b}$ is a square. Let $g \in \mathbb{F}_q^\times$ satisfy $g^2 = \frac{a}{b}$. By Proposition 1, there exist $x_0, y_0 \in \mathbb{F}_q$ such that $\frac{c}{a} = x_0^2 + y_0^2$. Set $y_1 = y_0 g$. Then

$$c = ax_0^2 + ay_0^2 = ax_0^2 + a\left(\frac{y_1}{g}\right)^2 = ax_0^2 + by_1^2. \qquad \blacksquare$$

There is a more straightforward argument than Weber's. Long before Weber's textbook was published, Cauchy [1] had solved Problem 2 when $d = 2$:

Second Proof of Proposition 2. If $\mathbb{F}_q$ has characteristic 2, then, as observed before, every element is already a square, which quickly finishes the argument. Otherwise, fix $a, b \in \mathbb{F}_q^\times$ and let $c \in \mathbb{F}_q$. Since there are $\frac{q+1}{2}$ squares in $\mathbb{F}_q$ and the cardinality of a subset of a finite field is invariant under multiplication or addition by a fixed nonzero element of the field, the sets $\{ax^2 : x \in \mathbb{F}_q\}$ and $\{c - by^2 : y \in \mathbb{F}_q\}$ both have cardinality $\frac{q+1}{2}$, i.e., occupy slightly more than half of the field $\mathbb{F}_q$. Thus these two sets have at least one common element z, which satisfies $z = ax^2 = c - by^2$ for some $x, y \in \mathbb{F}_q$. Hence, $c = ax^2 + by^2$. $\qquad \blacksquare$

Remark. Cauchy's argument is more well known than Weber's, in part because it has been rediscovered more frequently. See, e.g., [6, Lemma 1], where it appears without citation, perhaps because it was well known by then.

Cauchy's argument cannot be generalized to solve Problem 2 in general, not even when $d = 3$. For example, in $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, the set of cubes is $\{x^3 : x \in \mathbb{F}_7\} = \{0, 1, 6\}$, which has less than half the cardinality of the field. Thus, the pigeonhole principle used in the proof does not apply, as we cannot hope to intersect two modified sets of cubes. While we are here, we also observe that $\{x^3 + y^3 : x, y \in \mathbb{F}_7\} = \{0, 1, 2, 5, 6\} \neq \mathbb{F}_7$, so the failure of the argument is of course caused by $\mathbb{F}_7$ itself and not by a lack of ingenuity in modifying the technique in some way.

It turns out that, except when $q = 4$ and $q = 7$, every element of $\mathbb{F}_q$ can be written as a sum of two cubes, which solves Problem 1 in the case $d = 3$. This precise result, proved in an elementary way in the twentieth century, is due to Skolem[6] [27] when q is prime and to Singh [26] in general. Skolem and many others addressed Problem 2 in the case $d = 3$; see [20, pp. 325–326] for sources.

Diverting our attention from successes of elementary methods for the moment, we return to the nineteenth century. Initiating the study of cyclotomy,[7] a web of

---

[6]Unlike these other people, who did not help found finitism, Skolem was more keen on mathematical logic. Several of his results, including this one, were independently rediscovered due to the general disconnection in research networks that prevailed in the years before the internet.

[7]See [30] for a treatment of cyclotomy.

problems that all involve roots of unity, Gauss, according to Weil, "obtain[ed] the numbers of solutions for all congruences $ax^3 - by^3 \equiv 1 \pmod{p}$" for primes p with $p \equiv 1 \pmod 3$ and "[drew] attention himself to the elegance of his method, as well as to its wide scope" [**33**]. Weil adds that V. A. Lebesgue (and, by implication, Gauss as well) was unable to bring these vaunted methods to bear on the full generality of Problem 3. We remark that V. A. Lebesgue and others had modest successes on specific cases with the same flavor as the quoted result by Gauss—restricted to q prime, and so on. It was Kummer who more securely connected cyclotomy to Gauss sums [16–18], paving the way for further advancements in the theory of diagonal equations.

We enter the twentieth century again, this time wearing our cyclotomy goggles. From this viewpoint, Dickson was quite important. The following theorem of his, from two of dozens of his cyclotomy papers, illustrates another historical reason for interest in diagonal equations:

Theorem 1 ([4, 5]). *Fix an odd prime $e > 2$. Then for all sufficiently large primes p, the equation*

$$x^e + y^e + z^e = 0 \pmod{p} \tag{2}$$

has a solution $(x, y, z) \in (\mathbb{F}_p^\times)^3$.

Remark. This theorem's *raison d'être* was that it nullified an approach to proving the case of Fermat's last theorem with prime exponents. If the conclusion of Theorem 1 were false for, say, $e = 3$, then there would exist a sequence of primes (p_n) tending to infinity for which the only solutions $(x, y, z) \in \mathbb{F}_{p_n}^3$ to equation (2) with $e = 3$ would have at least one of x, y, z divisible by p_n. It follows that if we had a solution in integers to the equation $x^3 + y^3 + z^3 = 0$, taking this equation modulo a large enough p_n would yield a contradiction. Perhaps surprisingly, this observation appears in [**11**], but not [**4**] or [**5**].

As stated, Theorem 1 is a partial solution to Problem 3 but not to Problem 2 or even Problem 1. Hurwitz obtained an improvement which pertains to Problem 2:

Theorem 2 ([11]). *Fix an odd prime $e > 2$ and nonzero integers $a, b,$ and c. Then for all sufficiently large primes p, the equation*

$$ax^e + by^e + cz^e = 0 \pmod{p} \tag{3}$$

has a solution $(x, y, z) \in (\mathbb{F}_p^\times)^3$.

Remark. If p is a prime such that $(x, y, z) \in (\mathbb{F}_p^\times)^3$ is a solution to equation (3), then after subtracting cz^e from both sides and dividing by z^e, we have

$$a \left(\frac{x}{z} \right)^e + b \left(\frac{y}{z} \right)^e = -c,$$

which expresses an arbitrary nonzero element $-c$ of $\mathbb{F}_p$ as a member of the set $\{ax^e + by^e : x, y \in \mathbb{F}_p\}$. Thus Theorem 2 solves Problem 2 when q is prime and d is an odd prime. We will make use of this division trick again.

Having explained some partial solutions to Problem 3, and their connection to Problems 1 and 2 in the case q prime, it is reasonable to say that everything has been set in motion. In a few decades, some solutions to Problem 3 have emerged. In this article, we are not interested in the exact details of these solutions, but for completeness's

© THE MATHEMATICAL ASSOCIATION OF AMERICA [Monthly 128

sake, we mention that, broadly speaking, the approaches go either by Gauss sums, or by Jacobi sums, or by elementary methods.[8]

Weil summarized historical progress on Problem 3 up to 1949 in [**33**], in the process simplifying and advancing some earlier work by Hasse and Davenport in [**2**]. It should be mentioned that the new results from [**33**] were discovered during the proofing process to be, in Weil's words, "substantially identical" to those of Hua and Vandiver [**9**] . What appears in [**33**] and [**9**] has been made more elementary in several presentations, such as [**12**], and can now be readily studied therefrom.

Small explicitly observed in the short article [**28**] the fact that a certain estimate on the number of solutions to diagonal equations yields a solution to Problem 1. For the sake of review, we now reproduce the one theorem from [**28**], with minor changes in notation for consistency:

Theorem 3 ([28]). *Let d be a positive integer, let $\mathbb{F}_q$ be a finite field, and put $\delta = \gcd(q - 1, d)$. Assume $q > (\delta - 1)^4$. Then every element of $\mathbb{F}_q$ is a sum of two dth powers. (In particular, the conclusion holds if $q > (d - 1)^4$, since $d \geq \delta$.)*

Proof. For $b \in \mathbb{F}_q$ let $N(b)$ denote the number of solutions $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ of $x^d + y^d = b$. Then, by definition, $N(b) \geq 0$; we have to show that $q > (\delta - 1)^4$ implies $N(b) > 0$. We may assume $b \neq 0$, since 0 is certainly a sum of two dth powers. Then, by [**13**, Corollary 1, p. 57], we have $|N(b) - q| \leq (\delta - 1)^2 \sqrt{q}$. In particular, $N(b) - q \geq -(\delta - 1)^2 \sqrt{q}$, so that $N(b) \geq \sqrt{q}(\sqrt{q} - (\delta - 1)^2)$. Hence, $N(b) > 0$, for all b, provided $\sqrt{q} > (\delta - 1)^2$, or in other words $q > (\delta - 1)^4$. ∎

Remark. If $d > 1$ is a fixed integer, one might wonder what is the largest integer q for which not every element of $\mathbb{F}_q$ is the sum of two dth powers. By Theorem 3, this value must be less than $(d - 1)^4 + 1$. This problem might be interesting to pursue, in part because it is related to Waring's problem over finite fields.

Small cites Jean-René Joly's self-contained survey [**13**] about equations and algebraic varieties over finite fields. In the chapter endnotes, Joly states that the particular result Small would later quote is due independently to Davenport and Hasse in a 1934 paper [**2**] and to Hua and Vandiver in 1949 papers [**9**] and [**10**]. But one of the Hua–Vandiver papers [**10**] cites [**2**] regarding the result in question![9] Anyway, as for the result Small uses, it follows from the development of Gauss and Jacobi sums over a few chapters in Joly.[10]

Remark. We remark that although Small recorded a solution to Problem 1, the inequality he quoted is general enough that he had essentially recorded a solution to Problem 2 as well.

In the remaining two sections, we share two other ways to attack Problem 2. The first is both new and elementary in the sense that it does not depend on Gauss sums, Jacobi sums, or hard counting of solutions to diagonal equations. As we will see, it is a soft averaging argument—what we are averaging will become apparent—and its main tool is the Cauchy–Schwarz inequality. The second way, which is not new, could

---

[8]Each of these methods, including a combined treatment of the elementary approaches by Stepanov [**29**] and Schmidt [**24**], is treated in, e.g., [**20**].

[9]It is possible that Hua and Vandiver [**9**] learned about the Davenport–Hasse [**10**] result after the publication in 1949 and before the publication of… in 1949. What a year 1949 was!

[10]The treatments in Joly [**13**] and Ireland–Rosen [**12**] are roughly equally accessible. After reading this paragraph and the one about Weil, the reader hopefully has some feeling of a frenzy, whether synchronous or asynchronous, around this topic.

accidentally be considered elementary if the reader blinks at the right moment. To be only a little more precise, we will reframe the situation using Fourier analysis, reducing the problem to a state where a single bolt of lightning from the Riemann hypothesis over finite fields creates a piece of fulgurite[11] to add to one's collection. We include this second approach as a byway to reiterate the continual importance of Fourier analysis and to emphasize a certain application from the high-minded theory of the Riemann hypothesis over finite fields, which we do not intend to explain here. We hope this will prove a useful juxtaposition with our elementary first proof and the arguments in this introduction.

2. AN ELEMENTARY APPROACH. From this section onward, we let μ_q denote the counting measure on $\mathbb{F}_q$, normalized to be a probability measure; thus, for any subset A of $\mathbb{F}_q$, $\mu_q(A)$ equals $|A|/q$, the cardinality of A divided by q. In context, q will be fixed, so we will suppress the subscript and just write μ. Besides measuring sets, we will also shift them: If y lives in $\mathbb{F}_q$, denote by $A + y$ the set

$$A + y := \{x + y \in \mathbb{F}_q : x \in A\}.$$

We need a basic lemma.

Lemma 1. *Fix positive integers d and q, and let $\delta = \gcd(d, q - 1)$. Then*

$$\{x^\delta : x \in \mathbb{F}_q\} = \{x^d : x \in \mathbb{F}_q\}.$$

Proof. By Bézout's lemma, there exist integers r and s such that $rd + s(q - 1) = \delta$. Hence, for all $x \in \mathbb{F}_q^\times$, we have

$$x^\delta = (x^r)^d (x^s)^{q-1} = (x^r)^d, \tag{4}$$

since $y^{q-1} = 1$ for all $y \in \mathbb{F}_q^\times$. But equation (4) implies the set containment

$$\{x^\delta : x \in \mathbb{F}_q\} \subseteq \{x^d : x \in \mathbb{F}_q\}.$$

The reverse set containment holds since $x^d = (x^{d/\delta})^\delta$ for all $x \in \mathbb{F}_q$. ∎

Now, as promised in the introduction, we provide here an elementary proof of the following:

Theorem 4. *Fix an integer $d > 1$. Then, for every sufficiently large finite field $\mathbb{F}_q$ with characteristic larger than d and every $a, b \in \mathbb{F}_q^\times$, we have*

$$\mathbb{F}_q = \{ax^d + by^d : x, y \in \mathbb{F}_q\}.$$

Remark. If we restrict to the special case where q is prime, we can remove the assumption that $\text{char}(\mathbb{F}_q) > d$. Indeed, let $q = p$ be prime, let $d > 1$, and set $\delta = \gcd(d, p - 1)$. By Lemma 1, it follows that

$$\{ax^d + by^d : x, y \in \mathbb{F}_p\} = \{ax^\delta + by^\delta : x, y \in \mathbb{F}_p\}$$

for all $a, b \in \mathbb{F}_p^\times$. The result follows from the theorem since $\delta < p = \text{char}(\mathbb{F}_p)$.

To prove Theorem 4, we will first need to state two lemmas. We prove the easier one immediately and defer the proof of the other one to the end of the section.

---

[11]Fulgurite is a general term for a mineral-like clump of dirt that can form where lightning strikes the ground.

Lemma 2. *Fix a finite field $\mathbb{F}_q$ and an integer $d > 1$, and let $A = \{x^d : x \in \mathbb{F}_q\}$. Then $\mu(A) > \frac{1}{d}$.*

Proof. The map $\phi : \mathbb{F}_q^\times \to \mathbb{F}_q^\times$ given by $\phi(x) = x^d$ is a group homomorphism. Since the equation $x^d = 1$ has at most d distinct solutions in $\mathbb{F}_q$, it follows that $|\ker(\phi)| \leq d$. Thus

$$|A| - 1 \;=\; |\mathrm{im}(\phi)| \;=\; \frac{|\mathbb{F}_q^\times|}{|\ker(\phi)|} \;=\; \frac{q-1}{|\ker(\phi)|} \;\geq\; \frac{q-1}{d},$$

which implies that

$$|A| \;\geq\; 1 + \frac{q-1}{d} \;>\; \frac{1}{d} + \frac{q-1}{d} \;=\; \frac{q}{d}.$$

Thus $\mu(A) = \frac{|A|}{q} > \frac{1}{d}$. ∎

Lemma 3. *There is a positive function $\mathcal{E}(q, d) : \mathbb{N}^2 \to \mathbb{R}$ with these properties:*

1. *For any q, any subsets $A_q, B_q \subseteq \mathbb{F}_q$, and any polynomial $P \in \mathbb{F}_q[x]$ with degree d satisfying $1 < d < \mathrm{char}(\mathbb{F}_q)$, we have*

$$\left| \frac{1}{q} \sum_{g \in \mathbb{F}_q} \mu(A_q \cap (B_q + P(g))) - \mu(A_q)\mu(B_q) \right| \;\leq\; \mathcal{E}(q, d). \tag{5}$$

2. *For any fixed d, we have $\lim_{q \to \infty} \mathcal{E}(q, d) = 0$.*

Remarks. 1. In the first statement, we suppose $d > 1$ because Problems 1 and 2 are trivially solved without this lemma when $d = 1$. In fact, for polynomials P of degree 1, the left-hand side of (5) is always 0. On the other hand, it is not possible to remove the assumption that $d < \mathrm{char}(\mathbb{F}_q)$. This is because for certain choices of P, for example $P(x) = x^{\mathrm{char}(\mathbb{F}_q)} + x$, the supremum over A_q and B_q of the left-hand side of (5) is bounded away from 0, independently of q.

2. This lemma asserts that, eventually, the quantities $\mu(A_q \cap (B_q + P(g)))$ are of size $\mu(A_q)\mu(B_q)$ on average. We will see in the proof of Theorem 4 that, when concrete choices of A_q and B_q are made, this currently vague statement will suddenly reveal useful information, namely the nontrivial intersection of A_q and $B_q + P(g)$ for some $g \neq 0$.

3. Our choice of $\mathcal{E}(q, d)$ will not be optimal in any reasonable sense.

Proof of Theorem 4. We need only to show that $\mathbb{F}_q \subseteq \{ax^d + by^d : x, y \in \mathbb{F}_q\}$, as the reverse inclusion is trivial. Let $A_q = \{ax^d : x \in \mathbb{F}_q\}$ and $B_q = \{-by^d : y \in \mathbb{F}_q\}$. Fix $c \in \mathbb{F}_q^\times$, and let $P(x) = cx^d$. Let $\mathcal{E}(q, d)$ be the function from Lemma 3.

Claim. For sufficiently large q, we have

$$\mu(A_q)\mu(B_q) - \frac{1}{q}\mu(A_q \cap B_q) \;>\; \mathcal{E}(q, d).$$

Indeed, by Lemma 2, $\mu(A_q) > \frac{1}{d}$ and $\mu(B_q) > \frac{1}{d}$. Since $\lim_{q \to \infty} \mathcal{E}(q, d) = 0$ and $\frac{1}{q}\mu(A_q \cap B_q) \leq \frac{1}{q}$, it follows that for sufficiently large q we have

$$\mathcal{E}(q, d) + \frac{1}{q}\mu(A_q \cap B_q) \;<\; \frac{1}{d^2} \;<\; \mu(A_q)\mu(B_q),$$

whence the claim.

Now, define the closely related quantities

$$S = \frac{1}{q} \sum_{g \in \mathbb{F}_q} \mu(A_q \cap (B_q + P(g))) \quad \text{and}$$

$$T = \frac{1}{q} \sum_{g \in \mathbb{F}_q^\times} \mu(A_q \cap (B_q + P(g))).$$

We note that $S = T + \frac{1}{q}\mu(A_q \cap B_q)$, which follows by adding the missing $g = 0$ term to T.

For sufficiently large q, Lemma 3 implies that

$$S - \mu(A_q)\mu(B_q) \geq -\mathcal{E}(q, d). \tag{6}$$

Thus, for sufficiently large q, it follows by the claim and (6) that

$$T = S - \frac{1}{q}\mu(A_q \cap B_q)$$

$$= \left(S - \mu(A_q)\mu(B_q)\right) + \left(\mu(A_q)\mu(B_q) - \frac{1}{q}\mu(A_q \cap B_q)\right)$$

$$> -\mathcal{E}(q, d) + \mathcal{E}(q, d) = 0.$$

Since $T > 0$ and T is a sum of nonnegative numbers, at least one summand is positive. Thus, there is an element $g \in \mathbb{F}_q^\times$ such that $\mu(A_q \cap (B_q + P(g))) > 0$. Having positive measure, the set $A_q \cap (B_q + P(g))$ must therefore be nonempty; hence there exist $x_1, x_2 \in \mathbb{F}_q$ such that $ax_1^d = -bx_2^d + cg^d$. Since $g \neq 0$, we can rearrange[12] this equation to yield

$$c = a\left(\frac{x_1}{g}\right)^d + b\left(\frac{x_2}{g}\right)^d,$$

which shows that $c \in \{ax^d + by^d : x, y \in \mathbb{F}_q\}$. But $c \in \mathbb{F}_q^\times$ was arbitrary, and of course $0 = a \cdot 0^d + b \cdot 0^d$; hence we are done. ∎

To prove the lemma that has done all the heavy lifting for us, we need some elementary facts about inner products. Fix a finite field $\mathbb{F}_q$. Define the inner product

$$\langle f_1, f_2 \rangle := \int_{\mathbb{F}_q} f_1 \overline{f_2} \, d\mu = \frac{1}{q} \sum_{g \in \mathbb{F}_q} f_1(g) \overline{f_2(g)}$$

for functions $f_1, f_2 : \mathbb{F}_q \to \mathbb{C}$ and write the corresponding norm $||f_1|| := \sqrt{\langle f_1, f_1 \rangle}$. In this notation, the Cauchy–Schwarz inequality has a simple form:

$$|\langle f_1, f_2 \rangle| \leq ||f_1|| \cdot ||f_2||. \tag{7}$$

Indeed, for $a_1, \ldots, a_q, b_1, \ldots, b_q \in \mathbb{C}$, the Cauchy–Schwarz inequality states that

$$\left|\sum_{i=1}^{q} a_i \overline{b_i}\right|^2 \leq \sum_{j=1}^{q} |a_j|^2 \sum_{k=1}^{q} |b_k|^2. \tag{8}$$

---

[12]We have encountered this trick before. In the introduction, it appeared in the remark that explains how Theorem 2 solves Problem 2 when q is prime.

© THE MATHEMATICAL ASSOCIATION OF AMERICA

Setting[13] $a_j = f_1(j)$ and $b_k = f_2(k)$ and dividing both sides by q^2, we obtain

$$\left| \frac{1}{q} \sum_{i=1}^{q} f_1(i) \overline{f_2(i)} \right|^2 \leq \left(\frac{1}{q} \sum_{j=1}^{q} |f_1(j)|^2 \right) \left(\frac{1}{q} \sum_{k=1}^{q} |f_2(k)|^2 \right),$$

which is written compactly as $|\langle f_1, f_2 \rangle|^2 \leq \langle f_1, f_1 \rangle \langle f_2, f_2 \rangle$, whence (7).

All the functions we will take inner products with will be real-valued, so we will treat this inner product as a pleasantly linear tool. In particular, we will pull finite sums in and out, without warning.

Proof of Lemma 3. Fix q and subsets $A, B \subseteq \mathbb{F}_q$. In the proof of Theorem 4 we only used polynomials of the form $P(x) = cx^d$ for $c \in \mathbb{F}_q$ nonzero, so we will stick with these for illustration.

If 1_A is the characteristic function of A, let a_g be the function $\mathbb{F}_q \to \mathbb{C}$ defined by $x \mapsto 1_A(x + g) - \mu(A)$. We make two observations about these a_g's, both involving shifts, and both justifying the utility of this weird function. First, after a change of variable $x \mapsto x - g'$, we see

$$\langle a_g, a_{g'} \rangle = \int_{\mathbb{F}_q} \Big(1_A(x + g) - \mu(A) \Big) \Big(1_A(x + g') - \mu(A) \Big) \, d\mu(x)$$

$$= \int_{\mathbb{F}_q} \Big(1_A(x + g - g') - \mu(A) \Big) \Big(1_A(x) - \mu(A) \Big) \, d\mu(x)$$

$$= \langle a_{g-g'}, a_0 \rangle. \tag{9}$$

Second, one checks[14] that

$$\langle a_{P(g)}, 1_B \rangle = \int_{\mathbb{F}_q} (1_A(x + P(g)) - \mu(A)) \, 1_B(x) \, d\mu(x)$$

$$= \int_{\mathbb{F}_q} \Big(1_{A-P(g)}(x) - \mu(A) \Big) \, 1_B(x) \, d\mu(x) \tag{10}$$

$$= \int_{\mathbb{F}_q} \Big(1_{A-P(g)}(x) 1_B(x) - \mu(A) 1_B(x) \Big) \, d\mu(x)$$

$$= \int_{\mathbb{F}_q} \Big(1_{(A-P(g)) \cap B}(x) - \mu(A) 1_B(x) \Big) \, d\mu(x) \tag{11}$$

$$= \mu((A - P(g)) \cap B) - \mu(A)\mu(B),$$

---

[13] We are effectively enumerating the elements of $\mathbb{F}_q$ as $g_1, \ldots, g_q$ and writing $f_1(j)$ instead of $f_1(g_j)$. This abuse of notation is committed only to clarify how one form of Cauchy–Schwarz follows from another.

[14] Equation (10) holds since $x + y \in A$ if and only if $x \in A - y$, and (11) since $1_A(x) 1_B(x) = 1_{A \cap B}(x)$.

so that

$$\langle a_{P(g)}, 1_B \rangle = \mu(A \cap (B + P(g))) - \mu(A)\mu(B). \tag{12}$$

With the help of equation (12), we begin. By Cauchy–Schwarz, we have

$$\left| \frac{1}{q} \sum_{g \in \mathbb{F}_q} \mu(A \cap (B + P(g))) - \mu(A)\mu(B) \right| = \left| \left\langle \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g)}, 1_B \right\rangle \right|$$

$$\leq \left\| \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g)} \right\| \cdot \|1_B\|$$

$$\leq \left\| \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g)} \right\|, \tag{13}$$

where we used the fact that $\|1_B\| = \sqrt{\langle 1_B, 1_B \rangle} = \sqrt{\mu(B)} \leq 1$.

We prepare to bound the norm in (13) using the following elementary observation. Namely, if $h \in \mathbb{F}_q$ is fixed, the polynomial

$$P(x + h) - P(x) = c(x + h)^d - cx^d$$

has degree at most $d - 1$ in x. Usually the degree will be $d - 1$, but it can be smaller if $h = 0$ or if we did not suppose the characteristic of $\mathbb{F}_q$ is larger than d. This *differencing* procedure allows us to reduce the degree of a polynomial whenever we can introduce this difference, which we will do aggressively.[15] If we are given parameters $h_1, h_2, \ldots, h_{d-1} \in \mathbb{F}_q$, let

$$P(x; h_1) := P(x + h_1) - P(x),$$

$$P(x; h_1, h_2) := P(x + h_2; h_1) - P(x; h_1),$$

$$\vdots$$

$$P(x; h_1, h_2, \ldots, h_{d-1}) := P(x + h_{d-1}; h_1, h_2, \ldots, h_{d-2}) - P(x; h_1, h_2, \ldots, h_{d-2})$$

be, respectively, the degree at most $d - 1$, degree at most $d - 2$, ..., and degree at most 1 polynomials in x obtained by consecutively differencing P by h_1, then the result by h_2, and so on down to a (usually) linear polynomial. Now we return to bound the norm in (13). This is a key step.

Observe, after using the first fact (9) about the a_g's, reindexing a sum to introduce differencing, and applying the triangle and Cauchy–Schwarz inequalities,

$$\left\| \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g)} \right\|^2 = \left\langle \frac{1}{q} \sum_{g' \in \mathbb{F}_q} a_{P(g')}, \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g)} \right\rangle \qquad \text{by definition}$$

$$= \frac{1}{q} \sum_{g' \in \mathbb{F}_q} \frac{1}{q} \sum_{g \in \mathbb{F}_q} \langle a_{P(g')}, a_{P(g)} \rangle$$

---

[15] Arguably the most notable use of this idea is in [**34**], wherein Weyl shows that if $Q(x)$ is a real polynomial with at least one irrational coefficient, then $\{Q(n) : n \in \mathbb{N}\}$ is uniformly distributed modulo 1.

$$= \frac{1}{q} \sum_{g' \in \mathbb{F}_q} \frac{1}{q} \sum_{g \in \mathbb{F}_q} \langle a_{P(g')-P(g)}, a_0 \rangle \qquad \text{by (9)}$$

$$= \frac{1}{q} \sum_{h_1 \in \mathbb{F}_q} \frac{1}{q} \sum_{g \in \mathbb{F}_q} \langle a_{P(g+h_1)-P(g)}, a_0 \rangle$$

$$= \frac{1}{q} \sum_{h_1 \in \mathbb{F}_q} \left\langle \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g;h_1)}, a_0 \right\rangle$$

$$\leq \frac{1}{q} \sum_{h_1 \in \mathbb{F}_q} \left\| \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g;h_1)} \right\|. \tag{14}$$

Note that the last step follows[16] since

$$\|a_0\| = \|1_A - \mu(A)\| = \sqrt{\mu(A) - \mu(A)^2} \leq 1.$$

This argument in (14) has reduced the degree of $P(g)$ by (at least) one. Encouraged, we prepare to iterate. For each h_1, making the displayed argument with $a_{P(g;h_1)}$ replacing $a_{P(g)}$ on the left-hand side, we get a bound on $\left\| \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g;h_1)} \right\|$ in terms of a new parameter h_2, which plays the same role as h_1 in the displayed argument. This yields

$$\left\| \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g;h_1)} \right\| \leq \sqrt{\frac{1}{q} \sum_{h_2 \in \mathbb{F}_q} \left\| \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g;h_1,h_2)} \right\|}. \tag{15}$$

Applying (15) to the norm in (14), we find

$$\left\| \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g)} \right\|^2 \leq \frac{1}{q} \sum_{h_1 \in \mathbb{F}_q} \sqrt{\frac{1}{q} \sum_{h_2 \in \mathbb{F}_q} \left\| \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g;h_1,h_2)} \right\|},$$

where $P(g; h_1, h_2) = P(g + h_2; h_1) - P(g; h_1)$ is a polynomial in g of degree at most $d - 2$ for each $h_1, h_2 \in \mathbb{F}_q$. Proceeding recursively in this way, we see that

$$\left\| \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g)} \right\|^2 \leq \frac{1}{q} \sum_{h_1 \in \mathbb{F}_q} \sqrt{\frac{1}{q} \sum_{h_2 \in \mathbb{F}_q} \sqrt{\cdots \sqrt{\frac{1}{q} \sum_{h_{d-2} \in \mathbb{F}_q} \left\| \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g;h_1,h_2,\ldots,h_{d-2})} \right\|}}}, \tag{16}$$

where $P(g; h_1, h_2, \ldots, h_{d-2})$ is the polynomial in g of degree at most 2 obtained by differencing. If we reduce the degree one more time—but without applying Cauchy–Schwarz—we will obtain an expression that we can finally bound. Indeed, by repeating the argument of (14), stopping just before the inequality, observe that for any $h_1, h_2, \ldots, h_{d-2} \in \mathbb{F}_q$, we have

---

[16]Note that $\|a_0\| = \sqrt{\mu(A) - \mu(A)^2} \leq \frac{1}{2}$ since the function $x \mapsto x - x^2$ has maximum $\frac{1}{4}$ on $[0, 1]$, but this better bound is not necessary for our argument.

$$\left\| \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g;h_1,\ldots,h_{d-2})} \right\|^2 = \frac{1}{q} \sum_{h_{d-1} \in \mathbb{F}_q} \left\langle \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g;h_1,h_2,\ldots,h_{d-1})}, a_0 \right\rangle. \quad (17)$$

By applying equation (17) to the innermost part of (16), we have

$$\left\| \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g)} \right\|^2 \leq \frac{1}{q} \sum_{h_1 \in \mathbb{F}_q} \sqrt{\cdots \sqrt{\frac{1}{q} \sum_{h_{d-1} \in \mathbb{F}_q} \left\langle \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g;h_1,h_2,\ldots,h_{d-1})}, a_0 \right\rangle}}. \quad (18)$$

After taking square roots on both sides of (18), we have an expression with $d - 1$ radical symbols in it, which is annoying to look at and, fortunately, possible to adjust. By a different form of Cauchy–Schwarz,[17] we can move each of the square roots to the outside of the expression. This massaging of radical symbols is not necessary for the argument, but we hope the reader will appreciate the service. The result is that

$$\left\| \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g)} \right\| \leq \left(\frac{1}{q^{d-1}} \sum_{h_1,\ldots,h_{d-1} \in \mathbb{F}_q} \left\langle \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g;h_1,h_2,\ldots,h_{d-1})}, a_0 \right\rangle \right)^{2^{-(d-1)}}. \quad (19)$$

Compare (19) and (13). To finish the proof of the lemma, the idea is that the inner product in (19) is zero most of the time, i.e., for enough choices of the parameters h_i, and if it's not zero, then it can be bounded trivially.

First, the popular case. Tracing what happens when one differences $P(g) = cg^d$ the whole $d - 1$ times, one sees that the linear coefficient of $P(g; h_1, \ldots, h_{d-1})$, viewed as a linear polynomial in g, is $d! c \prod_{i=1}^{d-1} h_i$. Since $d < \mathrm{char}(\mathbb{F}_q)$ and $c \neq 0$, this coefficient is zero if and only if at least one $h_i = 0$. Thus, for fixed nonzero $h_1, h_2, \ldots, h_{d-1} \in \mathbb{F}_q^\times$, this linear coefficient is invertible, which implies that the map $g \mapsto P(g; h_1, \ldots, h_{d-1})$ is a permutation of $\mathbb{F}_q$. Using this permutation to reindex a sum, we see that

$$\left\langle \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g;h_1,h_2,\ldots,h_{d-1})}, a_0 \right\rangle = \left\langle \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_g, a_0 \right\rangle,$$

and a straightforward calculation shows that the function

$$\frac{1}{q} \sum_{g \in \mathbb{F}_q} a_g(x) = \frac{1}{q} \sum_{g \in \mathbb{F}_q} 1_A(x + g) - \mu(A)$$

is the zero function, so that the inner product of interest is 0. Now, for the unpopular case, if any h_i is 0, then $P(g; h_1, \ldots, h_{d-1})$ is a constant polynomial in g, and after analyzing the differencing process, one can see that, in particular, the constant is 0. It follows that

$$\left\langle \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g;h_1,h_2,\ldots,h_{d-1})}, a_0 \right\rangle = \langle a_0, a_0 \rangle = ||a_0||^2 \leq 1.$$

---

[17]Namely, if $c_1, \ldots, c_q$ are positive numbers, then $\frac{1}{q} \sum_{i=1}^{q} \sqrt{c_i} \leq \sqrt{\frac{1}{q} \sum_{i=1}^{q} c_i}$. To see this, set $a_j = \sqrt{c_j}$ and $b_k = 1$ in (8), divide both sides by q^2, then take the square root of both sides. For the interested reader, this inequality is first applied with "$i = h_{d-2}$" and $c_i = \frac{1}{q} \sum_{h_{d-1} \in \mathbb{F}_q} \left\langle \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g;h_1,h_2,\ldots,h_{d-1})}, a_0 \right\rangle$, where we again only abuse notation when clarifying something related to Cauchy–Schwarz.

The final step is to reckon the exact popularity of the two cases. Of the q^{d-1} choices of parameters $(h_1, \ldots, h_{d-1})$, exactly $(q-1)^{d-1}$ of them have no h_i equal to zero. Thus, the unpopular case, comprising everything else, happens $q^{d-1} - (q-1)^{d-1}$ times in the sum in (19). It follows that

$$\left\| \frac{1}{q} \sum_{g \in \mathbb{F}_q} a_{P(g)} \right\| \leq \left(\frac{q^{d-1} - (q-1)^{d-1}}{q^{d-1}} \right)^{2^{-(d-1)}}.$$

Thus, take $\mathcal{E}(q, d) = \left(\frac{q^{d-1} - (q-1)^{d-1}}{q^{d-1}} \right)^{2^{-(d-1)}}$. For fixed d, $\lim_{q \to \infty} \mathcal{E}(q, d) = 0$. ∎

Recalling the remark below Theorem 4, we observe that Theorem 4 solves Problem 2 except for those nonprime finite fields with characteristic drawn from the set of primes less than or equal to d. For context, this solves more of Problem 2 than Hurwitz's Theorem 2 does, and less of Problem 2 than Theorem 3 does. We judge this to be a success of elementary methods. Indeed, a method as soft as this cannot be expected to compete directly with careful estimates of numbers of solutions to diagonal equations. On the other hand, the full details of this method fit in these pages easily, and demonstrate the staying power of Cauchy–Schwarz, of differencing, and of averaging.

3. A FOURIER-ANALYTIC APPROACH. The first approach was animated by an all-encompassing desire to reduce the degree of a polynomial until it is linear, because a linear polynomial behaves predictably with respect to the averages we have considered—compare the popular and unpopular cases above. The basic structure of the second approach is similar overall: an auxiliary lemma will do most of the work with the help of the same averaging argument. However, in contrast to the erstwhile insistence on differencing, the second approach tolerates polynomiality until it becomes a lightning rod. We will find under this electric influence that the second approach solves Problem 2 in full generality.

Preliminaries. We need just a little Fourier analysis.

An *additive character* of $\mathbb{F}_q$ is a homomorphism $\chi : (\mathbb{F}_q, +) \to \mathbb{C}^\times$. If $\mathbb{F}_q$ has characteristic p, then evidently $\chi(g)^p = \chi(pg) = \chi(0) = 1$ for any $g \in \mathbb{F}_q$, so χ actually takes values in the set of the pth roots of unity. As a result, we conclude that $\chi(-g) = \chi(g)^{-1} = \overline{\chi(g)}$. Of course, χ is an additive character if and only if $\overline{\chi}$ is. The *principal character* χ_0 is identically 1. The set $\widehat{\mathbb{F}_q}$ of additive characters of $\mathbb{F}_q$ is an orthonormal basis for the q-dimensional $\mathbb{C}$-linear space of functions $f : \mathbb{F}_q \to \mathbb{C}$ with the inner product $\langle \cdot, \cdot \rangle$ defined in the previous section. Hence, with a small amount of work on orthogonality of characters, one can show that any f can be written as a linear combination of additive characters in the following way:

$$f = \sum_{\chi \in \widehat{\mathbb{F}_q}} \langle f, \chi \rangle \, \chi. \tag{20}$$

The *Fourier transform* of f, written $\hat{f}$, is the function $\hat{f} : \widehat{\mathbb{F}_q} \to \mathbb{C}$ given by $\hat{f}(\chi) = q \langle f, \overline{\chi} \rangle = \sum_{g \in \mathbb{F}_q} f(g)\chi(g)$. Thus $\langle f, \chi \rangle = \frac{\hat{f}(\overline{\chi})}{q}$; plugging this into (20) and reindexing the sum yields the Fourier inversion formula, valid for all $a \in \mathbb{F}_q$:

$$f(a) = \sum_{\chi \in \widehat{\mathbb{F}_q}} \frac{\hat{f}(\overline{\chi})}{q} \chi(a) = \frac{1}{q} \sum_{\chi \in \widehat{\mathbb{F}_q}} \hat{f}(\chi)\chi(-a). \tag{21}$$

With some more work, one can show the Plancherel formula: For any $f_1, f_2 : \mathbb{F}_q \to \mathbb{C}$, we have $\left\langle \hat{f}_1, \hat{f}_2 \right\rangle = q \left\langle f_1, f_2 \right\rangle$, where on the left-hand side we mean the analogous inner product

$$\left\langle \hat{f}_1, \hat{f}_2 \right\rangle := \frac{1}{q} \sum_{\chi \in \widehat{\mathbb{F}_q}} \hat{f}_1(\chi) \overline{\hat{f}_2(\chi)}.$$

Fourier analysis is a huge topic; for a sample, the interested reader may consult [**8**, **14**, **25**].

The content. We will state a variant of Lemma 3, use it to solve Problem 2, and then prove it.

Lemma 4. *There is a positive function $\mathcal{E}(q, d) : \mathbb{N}^2 \to \mathbb{R}$ with these properties:*

1. *For any q, any subsets $A_q, B_q \subseteq \mathbb{F}_q$, and any polynomial $P \in \mathbb{F}_q[x]$ with degree d coprime to q, we have*

$$\left| \frac{1}{q} \sum_{g \in \mathbb{F}_q} \mu(A_q \cap (B_q + P(g))) - \mu(A_q)\mu(B_q) \right| \leq \mathcal{E}(q, d).$$

2. *For any fixed d, we have $\lim_{q \to \infty} \mathcal{E}(q, d) = 0$.*

Remarks. These comments are parallel to their corresponding comments under Lemma 3.

1. This lemma strengthens Lemma 3, since the set of polynomials appearing in the first statement contains the set of polynomials with degree between 1 and $\mathrm{char}(\mathbb{F}_q)$.
2. The intuitive assertion of this lemma remains the same as in Lemma 3; namely, the quantities $\mu(A_q \cap (B_q + P(g)))$ are eventually of size $\mu(A_q)\mu(B_q)$ on average. Moreover, the application of this lemma will be almost exactly the same.
3. Our choice of $\mathcal{E}(q, d)$ here will decay to zero more quickly than it did in Lemma 3, except when $d = 2$, in which case it agrees with the previous choice.

Solution to Problem 2. We may suppose $q > d$. For q such that d is coprime with q, the argument proceeds as in the proof of Theorem 4, with Lemma 4 replacing Lemma 3, and shows that for all sufficiently large q coprime to d, for all $a, b \in \mathbb{F}_q^\times$, we have

$$\mathbb{F}_q = \{ax^d + by^d : x, y \in \mathbb{F}_q\}. \tag{22}$$

Otherwise, namely, if $\gcd(d, q) > 1$, then by Lemma 1, we have

$$\{ax^d + by^d : x, y \in \mathbb{F}_q\} = \{ax^\delta + by^\delta : x, y \in \mathbb{F}_q\},$$

where $\delta = \gcd(d, q - 1)$. Now, δ divides $q - 1$, so δ and q are coprime. This completes the argument since d has finitely many factors. ∎

Proof of Lemma 4. Fix q, subsets $A, B \subseteq \mathbb{F}_q$, and a polynomial $P \in \mathbb{F}_q[x]$ with degree d coprime to q.

We rewrite the expression

$$\frac{1}{q} \sum_{g \in \mathbb{F}_q} \mu(A \cap (B + P(g)))$$

step by step. Recall that $\mu(S) = \frac{|S|}{q} = \frac{1}{q} \sum_{h \in \mathbb{F}_q} 1_S(h)$, that $1_{S \cap S'}(x) = 1_S(x)1_{S'}(x)$, and that $1_{S+y}(x) = 1_S(x - y)$ for any $x, y \in \mathbb{F}_q$ and $S, S' \subseteq \mathbb{F}_q$. Thus,

$$\frac{1}{q} \sum_{g \in \mathbb{F}_q} \mu(A \cap (B + P(g))) = \frac{1}{q} \sum_{g \in \mathbb{F}_q} \frac{1}{q} \sum_{h \in \mathbb{F}_q} 1_A(h) 1_B(h - P(g)).$$

Inverting using equation (21) with $f = 1_B$ and $a = h - P(g)$, we find

$$\frac{1}{q} \sum_{g \in \mathbb{F}_q} \frac{1}{q} \sum_{h \in \mathbb{F}_q} 1_A(h) 1_B(h - P(g)) = \frac{1}{q^3} \sum_{g, h \in \mathbb{F}_q} \sum_{\chi \in \widehat{\mathbb{F}_q}} 1_A(h) \widehat{1_B}(\chi) \chi(P(g) - h).$$

After separating $\chi(P(g) - h) = \chi(P(g))\chi(-h) = \chi(P(g))\overline{\chi}(h)$ and changing the order of summation, we notice the expression for the Fourier transform of 1_A evaluated at the character $\overline{\chi}$:

$$\frac{1}{q^3} \sum_{g, h \in \mathbb{F}_q} \sum_{\chi \in \widehat{\mathbb{F}_q}} 1_A(h) \widehat{1_B}(\chi) \chi(P(g) - h) = \frac{1}{q^3} \sum_{g, \chi} \chi(P(g)) \widehat{1_B}(\chi) \underbrace{\sum_{h \in \mathbb{F}_q} 1_A(h) \overline{\chi}(h)}_{= \widehat{1_A}(\overline{\chi})}.$$

After changing the order of summation again, we have

$$\frac{1}{q^3} \sum_{g, \chi} \chi(P(g)) \widehat{1_B}(\chi) \widehat{1_A}(\overline{\chi}) = \frac{1}{q^3} \sum_{\chi} \widehat{1_A}(\overline{\chi}) \widehat{1_B}(\chi) \sum_g \chi(P(g)).$$

Let's separate the $\chi = \chi_0$ term from the whole sum. Remember, χ_0 is identically 1. Thus, by definition, $\widehat{1_A}(\chi_0) = \sum_{g \in \mathbb{F}_q} 1_A(g) \chi_0(g) = \sum_{g \in \mathbb{F}_q} 1_A(g) = |A|$, and since $\overline{\chi_0} = \chi_0$, we have $\widehat{1_B}(\overline{\chi}) = |B|$. Moreover, $\sum_{g \in \mathbb{F}_q} \chi_0(P(g)) = q$. Now $\frac{1}{q^3} \cdot |A||B|q = \mu(A)\mu(B)$. Thus

$$\frac{1}{q^3} \sum_{\chi} \widehat{1_A}(\overline{\chi}) \widehat{1_B}(\chi) \sum_g \chi(P(g)) = \mu(A)\mu(B) + \frac{1}{q^3} \sum_{\chi \neq \chi_0} \widehat{1_A}(\overline{\chi}) \widehat{1_B}(\chi) \sum_g \chi(P(g)).$$

Thus, to prove the lemma, we are looking for a function $\mathcal{E}(q, d)$ to bound

$$\left| \frac{1}{q^3} \sum_{\chi \neq \chi_0} \widehat{1_A}(\overline{\chi}) \widehat{1_B}(\chi) \sum_{g \in \mathbb{F}_q} \chi(P(g)) \right|. \tag{23}$$

By the triangle inequality, (23) is bounded by

$$\frac{1}{q^3} \sum_{\chi \neq \chi_0} \left| \widehat{1_A}(\overline{\chi}) \right| \left| \widehat{1_B}(\chi) \right| \left| \sum_{g \in \mathbb{F}_q} \chi(P(g)) \right|. \tag{24}$$

At this point, we await the lightning. Transcribing some folklore spawned from his own work, Weil wrote down in a short note in 1948 the relationship between some

exponential sums and the Riemann hypothesis over finite fields [**32**]. The specific formulation we use here appears[18] (with minor notation adjustments) in Kowalski's notes on exponential sums [**15**, Theorem 3.2]:

Theorem 5. *Fix a polynomial $f \in \mathbb{F}_q[x]$ of degree d and a nontrivial additive character χ of $\mathbb{F}_q$. If $d < q$ and d is coprime to q, then*

$$\left| \sum_{g \in \mathbb{F}_q} \chi(f(g)) \right| \leq (d-1)\sqrt{q}.$$

This theorem applies readily to part of (24). Thus, we find that (24) is bounded by

$$\frac{(d-1)\sqrt{q}}{q^3} \sum_{\chi \neq \chi_0} \left| \widehat{1_A}(\overline{\chi}) \right| \left| \widehat{1_B}(\chi) \right|. \tag{25}$$

Our final step uses the Plancherel formula. In preparation, we massage part of (25) by padding it with the $\chi = \chi_0$ term and applying Cauchy–Schwarz to see that

$$\sum_{\chi \neq \chi_0} \left| \widehat{1_A}(\overline{\chi}) \right| \left| \widehat{1_B}(\chi) \right| \leq \sum_{\chi} \left| \widehat{1_A}(\overline{\chi}) \right| \left| \widehat{1_B}(\chi) \right|$$

$$\leq \left(\sum_{\chi} \left| \widehat{1_A}(\chi) \right|^2 \sum_{\chi'} \left| \widehat{1_B}(\chi') \right|^2 \right)^{\frac{1}{2}}$$

$$= \left(q^4 \mu(A)\mu(B) \right)^{\frac{1}{2}} \tag{26}$$

$$\leq q^2,$$

where (26) holds by Plancherel since

$$\sum_{\chi} \left| \widehat{1_A}(\chi) \right|^2 = q \langle \widehat{1_A}, \widehat{1_A} \rangle = q^2 \langle 1_A, 1_A \rangle = q^2 \mu(A).$$

Thus (25) is bounded by

$$\frac{(d-1)\sqrt{q}}{q^3} \cdot q^2 = \frac{d-1}{\sqrt{q}},$$

so take $\mathcal{E}(q, d) = \frac{d-1}{\sqrt{q}}$. Obviously $\lim_{q \to \infty} \mathcal{E}(q, d) = 0$ for fixed d. ∎

In this approach we depend on serious, now classical, knowledge about certain exponential sums, a definite step up in difficulty over Gauss sums. The interest in these kinds of exponential sums arose in part as an outgrowth of interest in the problems of cyclotomy and diagonal equations but has since taken on its own life in number theory. We have certainly not done justice to the Riemann hypothesis over finite fields here; it is a deep topic. For a historical perspective, see [**21**], and for a mathematical discussion see, for example, [**12**]. What we have done is examined several facets of a pretty problem, Problem 2, found in the same deposit as Fermat's last theorem.

---

[18]For an offline source, see [**23**, Theorem 2E] or [**24**, Theorem 2.5].

REFERENCES

[1] Cauchy, A.-L. (1813). Recherches sur les nombres. *J. Éc. polytech. Math.* 9: 99–116; *Oeuvres* (II), vol. 1, pp. 39–63, Paris: Gauthier-Villars, 1905.

[2] Davenport, H., Hasse, H. (1934). Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen. *J. Reine Angew. Math.* 172: 151–182.

[3] Dedekind, R., Weber, H. M. (1882). Theorie der algebraischen Functionen einer Veränderlichen. *J. Reine Angew. Math.* 92: 181–290.

[4] Dickson, L. E. (1909). On the congruence $x^n + y^n + z^n \equiv 0$ mod p. *J. Reine Angew. Math.* 135: 134–141.

[5] Dickson, L. E. (1909). Lower limit for the number of sets of solutions of $x^e + y^e + z^e \equiv 0$ mod p. *J. Reine Angew. Math.* 135: 181–188.

[6] Dickson, L. E. (1926/27). Ternary quadratic forms and congruences. *Ann. of Math. (2).* 28(1–4): 333–341.

[7] Dickson, L. E. (1928). Review of Robert Fricke's *Lehrbuch der Algebra*. *Bull. Amer. Math. Soc.* 34: 531.

[8] Hardy, G. H., Rogosinski, W. W. (2013). *Fourier Series*, revised ed. Mineola, NY: Dover.

[9] Hua, L. K., Vandiver, H. S. (1949). Characters over certain types of rings, with applications to the theory of equations in a finite field. *Proc. Nat. Acad. Sci. U.S.A.* 35: 94–99.

[10] Hua, L. K., Vandiver, H. S. (1949). On the nature of the solutions of certain equations in a finite field. *Proc. Nat. Acad. Sci. U.S.A.* 35: 481–487.

[11] Hurwitz, A. (1909). Über die Kongruenz $ax^e + by^e + cz^e \equiv 0$ mod p. *J. Reine Angew. Math.* 136: 272–292.

[12] Ireland, K., Rosen, M. (1990). *A Classical Introduction to Modern Number Theory*, 2nd ed. New York: Springer-Verlag.

[13] Joly, J.-R. (1973). Équations et variétés algébriques sur un corps fini. *Enseign. Math.* 19(2): 1–117.

[14] Körner, T. W. (1989). *Fourier Analysis*. New York: Cambridge Univ. Press.

[15] Kowalski, E. (2018). Exponential sums over finite fields: elementary methods. Available at: people.math.ethz.ch/%7Ekowalski/exp-sums.pdf

[16] Kummer, E. E. (1850). Allgemeine Reciprocitätsgesetze für beliebig hohe Potenzreste. *Monatsber. Königl. Akad. Wiss. Berlin* 1850: 154–165; *Collected Papers*, Vol. 1, pp. 345–357, Berlin: Springer-Verlag, 1975.

[17] Kummer, E. E. (1851). Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers. *J. Math. Pures Appl.* 16: 377–498; *Collected Papers*, Vol. 1, pp. 363–484. Berlin: Springer-Verlag, 1975.

[18] Kummer, E. E. (1852). Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen. *J. Reine Angew. Math.* 44: 93–146; *Collected Papers*, Vol. 1, pp. 485–538, Berlin: Springer-Verlag, 1975.

[19] Lagrange, J.-L. (1770). Démonstration d'un théorème d'arithmétique. *Nouv. Mémoires Acad. Roy. Berlin* 1770: 123–133; *Oeuvres*, Vol. 3, pp. 189–201, Paris: Gauthier-Villars, 1869.

[20] Lidl, R., Niederreiter, H. (1997). *Finite Fields*, 2nd ed. New York: Cambridge Univ. Press.

[21] Roquette, P. (2018). *The Riemann Hypothesis in Characteristic p in Historical Perspective*. Lecture Notes in Mathematics, Vol. 2222. Cham, Switzerland: Springer.

[22] Schappacher, N. On the history of Hilbert's twelfth problem: A comedy of errors. *Matériaux pour l'Histoire des Mathématiques au XXe Siècle*, Nice, 1996, Sémin. Congr. 3 (Société Mathématique de France, Paris, 1998), 243–273.

[23] Schmidt, W. (1976). *Equations over Finite Fields: an Elementary Approach*, 1st ed. Lecture Notes in Mathematics, Vol. 536. Berlin: Springer-Verlag.

[24] Schmidt, W. (2004). *Equations over Finite Fields: an Elementary Approach*, 2nd ed. Heber City, UT: Kendrick Press.

[25] Shakarchi, R., Stein, E. M. (2003). *Fourier Analysis: An Introduction*. Princeton, NJ: Princeton Univ. Press.

[26] Singh, S. (1973). Analysis of each integer as sum of two cubes in a finite integral domain. *Indian J. Pure Appl. Math.* 6(1): 29–35.

[27] Skolem, T. (1937). Zwei Sätze über kubische Kongruenzen. *Norske Vid. Selsk. Forh.* 10: 89–92.

[28] Small, C. (1977). Sums of powers in large finite fields. *Proc. Amer. Math. Soc.* 65(1): 35–36.

[29] Stepanov, S. A. (1994). *Arithmetic of Algebraic Curves*. New York: Springer.

[30] Storer, T. (1967). *Cyclotomy and Difference Sets*. Lectures in Advanced Mathematics, Vol. 2. Chicago, IL: Markham Publishing Co.

[31] Weber, H. M. (1899). *Lehrbuch der Algebra*, Vol. II, 3rd ed. Providence, RI: AMS Chelsea (reprint).

[32] Weil, A. (1948). On some exponential sums. *Proc. Nat. Acad. Sci. U.S.A.* 34: 204–207.

[33] Weil, A. (1949). Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.* 55: 497–508.

[34] Weyl, H. (1916). Über die Gleichverteilung von Zahlen mod. Eins. *Math. Ann.* 77(3): 313–352.

VITALY BERGELSON is a professor at the Ohio State University and a fellow of the American Mathematical Society. His research interests include ergodic theory and Ramsey theory.
Department of Mathematics, The Ohio State University, Columbus, OH 43210
bergelson.1@osu.edu

ANDREW BEST is a graduate student at the Ohio State University under the direction of V. Bergelson. His research is in ergodic Ramsey theory. He also enjoys playing badminton.
Department of Mathematics, The Ohio State University, Columbus, OH 43210
best.221@buckeyemail.osu.edu

ALEX IOSEVICH received his Ph.D. in 1993 under the direction of C. D. Sogge. He held positions at McMaster, Wright State, Georgetown, and Missouri before joining the faculty at the University of Rochester. Alex Iosevich is a Fellow of the American Mathematical Society, Class of 2014. He works in analysis, combinatorics, number theory and connections between these areas.
Department of Mathematics, The University of Rochester, Rochester, NY 14627
iosevich@math.rochester.edu